# Externe und applikationsinterne Autorisierung in OAuth2 Systemen

## Gliederung

1. Einleitung
2. Technische Grundlagen
   1. Erklärung grundlegender Begriffe
      1. Authentifizierung
      2. Autorisierung
      3. Integrität
      4. Authentizität
      5. Validierung
   2. OAuth2
      1. Rollen in OAuth2
         1. Resource Owner
         2. Resource Server
         3. Client
         4. Authorization Server
      2. Erhalt von Token
         1. Authorization Code Grant
         2. Refresh Token
   3. Rivest–Shamir–Adleman (RSA)
   4. JSON Web Token (JWT)
      1. JSON Web Key (JWK)
      2. JSON Web Signatur (JWS)
         1. RS256
   5. OpenID Connect
      1. ID Token
      2. Authorization Code Grant
   6. OAuth2 Endpunkte des Autorisationsservers
      1. Authorization Endpunkt
      2. Token Endpunkt
      3. JSON Web Key Set (JWKS) Endpunkt
   7. Zugriffskontrolle
      1. Role Based Access Control (RBAC)
      2. Attribute Based Access Control (ABAC)
3. Inhalt
   1. Systemarchitektur
      1. Authorization Server Keycloak
      2. Erhalt eines Tokens durch „Authorization Code Grant“ mit Postman
      3. Spring Boot
      4. Spring Security
         1. OAuth2 Resource Server
         2. Access Decision Manager
      5. Open Policy Agent (OPA)
      6. Testsystem 1: Autorisierung in Ressourceserver
      7. Testsystem 2: Autorisierung entkoppelt von Ressourceserver mit Open Policy Agent (OPA)
   2. Tests und Testtool
      1. Apache JMeter
         1. Testplan Performanz
            1. Anzahl Threads über Zeitraum X
            2. HTTP-Request Header mit Token
            3. Listener für Protokollierung von Testergebnissen

Graphische Darstellung der Round Trip Time

Statistische Protokollierung der Round Trip Time (Median, Mittelwert, Abweichung, Minimum, Maximum) und Datendurchsatz

* + - 1. Testplan Performanz 2
         1. Ansteigende Anzahl Threads über Zeitraum X
         2. Listener für Protokollierung von Testergebnissen

Graphische Darstellung der Round Trip Time

Berechnung der Steigung aus Grafik

* + - 1. Testplan Denial of Service
         1. Maximale Anzahl Threads über Zeitraum X
         2. HTTP-Request Header mit maximal großem Token
    1. Windows Ressource Monitor

1. Experimente
   1. Auswertung
      1. Apache JMeter Listeners Auswertung der RTT „Testplan Performanz 1“
         1. Median, Mittelwert, Abweichung, Minimum, Maximum der RTT
         2. Datendurchsatz
      2. Apache JMeter Listeners Auswertung der RTT „Testplan Performanz 2“
         1. Auswertung der Steigungen
      3. Windows Ressource Monitor
         1. CPU-Auslastung
         2. RAM-Belegung
2. Stand der Technik (Related Work) / Ausblick
   1. Neue Spezifikation für feinkörnige Autorisierung in OAuth2 in Arbeit - „OAuth 2.0 Rich Authorization Requests“
3. Zusammenfassung